UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE VEHICLE 2017 CADILLAC XT5 VIN: 1GYKNBRSXHZ106287

Case No. 7:24-mj-1164-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

as described in Attachment (A)

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment (B) hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422	Coercion and Enticement of a Minor
18 U.S.C. § 1470	Transfer of Obscene Materials to Minors

The application is based on these facts:

See attached affidavit which is attached hereto and incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jamie L. Smith
Applicant's signature

Jamie L. Smith, NCIS Special Agent
Printed name and title

On this day, Jamie Smith appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Application for a Search Warrant.

Date: July 8 2024

Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr., United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF: **THE VEHICLE 2017 CADILLAC XT5 VIN: 1GYKNBRSXHZ106287**	***FILED UNDER SEAL*** **Misc. No.** 7:24-mj-1164-RJ

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jamie Smith (Your Affiant), Special Agent with the U.S. Naval Criminal Investigative Service Resident Agency (NCISRA) Camp Lejeune, NC (CLNC) being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure to search the following (hereinafter collectively referred to as the "**TARGET LOCATION**"):

a. The vehicle **2017 CADILLAC XT5 VIN: 1GYKNBRSXHZ106287** (**"TARGET LOCATION"**), described in Attachment A, for evidence described in Attachment B; and

2. The **TARGET LOCATION** to be searched for evidence of violations of Title 18, United States Code, Section 2422 (Coercion and Enticement of a Minor) and Section 1470 (Transfer of Obscene Materials to Minors) (hereinafter referred to as the "TARGET OFFENSES"), more fully described in Attachments B.

AGENT BACKGROUND

3. I have been employed as a Special Agent with the Naval Criminal Investigative Service (NCIS) since July of 2022, and am currently assigned to the Family and Sexual Violence (F&SV) squad at Camp Lejeune, NC. I am routinely tasked to investigate violations of the Uniform

Code of Military Justice (UCMJ) and Federal statutes. These types of violations include crimes against persons, such as death investigations, sexual assaults, and crimes against children to include child sexual abuse and child exploitation that have a Department of the Navy (DON) or Department of Defense (DoD) nexus. I have gained experience through training and everyday work relating to conducting these types of investigations. I have also successfully completed the NCIS Special Agent Basic Training Integrated (SABTI) course held at the Federal Law Enforcement Training Center (FLETC). Prior to employment with NCIS, I was employed by the Defense Counterintelligence and Security Agency as a Counterintelligence analyst. I was responsible for conducting intelligence analysis, threat hunting in the cyber domain, and network analysis in support of critical technology protection for the Department of Defense.

4. As a Special Agent with NCIS, I have conducted numerous investigations which required the execution of Search Warrants, including those for online accounts, such as email accounts, online storage accounts and other online communication accounts, to locate and identify items of evidence. During these investigations, I have conducted follow up interviews, interrogations, and other necessary investigative endeavors. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. The statements in this affidavit are based in part on information and reports provided by NCIS and other law enforcement, and on my experience and background as a Special Agent with NCIS. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe

that evidence, fruits, and instrumentalities of the violations of the TARGET OFFENSES are located within the **TARGET LOCATION**.

6. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

DEFINITIONS

1. The following definitions apply to this Affidavit and Attachment B to this Affidavit.

2. "Visual depictions" include undeveloped film and videotape and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C.§ 2256(5).

3. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

4. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether -in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records; painting, typing) or electrical, electronic or magnetic form (including but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard

disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices, portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

5. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

6. Based on my training and experience, I will use the following technical terms to convey the following meanings:

a. *Cellular telephone*: A cellular telephone (or cellular phone or smartphone or mobile telephone, or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/ receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Cloud-based storage service*: as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and

laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

c. *Computer*: The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

d. *Computer Hardware*: The term "computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. *Computer Passwords and Data Security Devices*: The term "computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. *Electronic Communication Service ("ESP")*: as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

h. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

i. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. *SIM card*: A Subscriber Identity Module, or SIM, is an integrated circuit chip, or electronic storage device, that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contacts on many SIM cards. A SIM card contains its unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking code (PUK) for PIN unlocking.

k. *Storage Medium*: The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

24. Based on my training, experience, and research, I know that electronic devices and computer devices have capabilities that allow them to serve as a wireless telephone, digital camera, and portable media player. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

PROBABLE CAUSE

25. NCISRA Camp Lejeune Family and Sexual Violence squad conducted an online proactive operation targeting the sexual exploitation of children. During the operation, an individual communicated with an undercover agent (UCA1) via responding to an advertisement on the website Craigslist. Craigslist is an online

website and mobile application for posting classified advertisements. Postings are available in a wide range of categories, to include items for sale, house listings, and job advertisements. On 30Apr24, an individual, later identified as MARTY LEE KAMINSKI, responded to the advertisement. Below is a representative example of the messages exchanged between UCA1 and MARTY LEE KAMINSKI (MK) via Craigslist:

30APR24-01MAY24

MK: "I'm not the guy you met but I'm interested. I'm 71 MWM wife has not touched me n 16 years. Looking for a regular thing."

UCA1: "Hey! I think we can help with that. What is it that you're looking for? We are very open minded."

MK: "Thanks for replying my name is Marty I'm starving for affection. I enjoy pleasing more than being pleased. I'm not looking for a one time thing. I love to touch and make you feel good I enjoy lots of body contact and making out."

MK: "Any age is fine with me"

UCA1: "Okay, if you would like to talk more you can text me."

26. UCA1 proceeded to provide MARTY LEE KAMINSKI with their cellphone number to continue the conversation. MARTY LEE KAMINSKI initiated contact with UCA1 via text message from cellphone number (910) 330-9721. Database checks revealed the aforementioned phone number as being associated to a Verizon Wireless user by the name of MARTY LEE KAMINSKI with a date of birth of 05FEB53 and a location of Jacksonville, NC. Additionally, database checks revealed MARTY LEE

KAMINSKI was associated with the address 402 Brookeview Drive, Jacksonville, NC 28540, and a 2017 CADILLAC XT5 bearing North Carolina Disabled Veteran tag "946T DV" and VIN: 1GYKNBRSXHZ106287. The latest registration date for the aforementioned vehicle was listed as 02Oct23 with an expiration date of 30Sep24.

27. Additional publicly available and law enforcement database queries were conducted which revealed a possible email account of "oppie1953@gmail.com" associated with MARTY LEE KAMINSKI. Queries also revealed a YouTube account potentially associated with MARTY LEE KAMINSKI with the username "Poppie1953". This account had one visible subscription to channel "n5jms1005". The "n5jms1005" account appeared to have several tutorial videos for "SCANCAT Lite Plus" downloadable software, which allows the user to monitor police frequencies via their computer to potentially evade law enforcement.

28. MARTY LEE KAMINSKI later disclosed to UCA1 he would be interested in sexual intercourse with UCA1's 14-year-old step-daughter. Following the conversation with UCA1, MARTY LEE KAMINSKI began communicating via text message with a second UCA (UCA2) who he believed to be the 14-year-old female. Between 01MAY24 and 12JUN24, MARTY LEE KAMINSKI regularly communicated with UCA1 and UCA2 and detailed specific sexual acts he intended to participate in with UCA2.

29. Below is a representative example of the messages exchanged between MARTY LEE KAMINSKI (MK) and UCA1 and UCA2; however, does not represent all messages in the exact order they occurred between UCAs and MARTY LEE KAMINSKI (MK).

01MAY24

Conversation between UCA1 and MARTY LEE KAMINSKI (MK) via text message:

MK: "Hello I'm Marty"

UCA1: *smiley face emoji*

UCA1: "Hi Marty, my name is Samantha. Thanks for texting. It's a lot easier!"

MK: "I want you Samantha"

UCA1: "Well I am really looking for someone that could help my step daughter"

MK: "In what way?"

UCA1: "She's getting older and has expressed she's interested in things"

MK: "I would love to help her in any way that I can. How old is she?"

UCA1: "Kaylee is 14"

MK: "I would be very gentle and slow. Nothing to make her feel uncomfortable"

MK: "Has she ever played with a toy?"

UCA1: "No toys yet, she's 14 but has been asking a lot of questions"

UCA1: "Would you be okay with it? Or done it before. She trusts me."

MK: "I'm okay with it"

MK: *image of a pink vibrator sex toy in a box*

MK: "I would use it externally"

UCA1: "Okay, I'm going to talk to her about it. Can you go over how you want to use the toys so I can go over it with her?"

MK: "I would start with using the toy her breast I would slip my hand under her top gently playing with her nipples then move my hand down to her kitty using the toy and my hand. Listen to her moaning"

MK: "Has she experienced an erection? Would you like a picture to show her?"

UCA1: "What should I explain to her where her kitty is? She calls it something different…"

MK: *two images of an adult male penis*

MK: "What does she call it?

UCA1: "Well do you mean her vagina?"

MK: "Yes"

UCA1: "I want her to be as comfortable as possible"

MK: "Me too"

30. UCA1 proceeded to send MARTY LEE KAMINSKI a phone number for UCA2 who he believed to be the 14-year-old step-daughter of UCA1.

01MAY24

Conversation between MARTY LEE KAMINSKI (MK) and UCA2 via text message:

MK: "Do you play with yourself"

UCA2: "Play with myself how"

MK: "Touch your cookie"

MK: "Is there a certain spot down there that feels really good when you rub it?"

UCA2: "idk lol ive never rubbed down there before"

MK: "Oh my would you like for me to touch you down there?"

MK: 'Would you lay on your stomach and let me give you a nice tender massage"

UCA2: "if you want lol where would massage me"

MK: "On your shoulders back and your butt"

MK: "I have a toy that vibrates and would like to use it to tickle your back"

UCA2: "oh really? What kinda toy is is"

MK: "Would you like to see a picture of it?"

UCA2: "yea sure"

MK: *two images depicting a pink vibrator sex toy in a box*

UCA2: "oh that looks like the pic my mom showed me lol"

MK: "it is"

MK: "I would like to touch your cookie with it"

UCA2: "I mean if u wanna"

MK: "I bet it would feel very nice I would like to see you cum"

02MAY24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:

MK: "Do you enjoy kissing?"

UCA2: "yea I guess I kissed a boy before"

MK: "Oh okay would you mind if I kissed you"

UCA2: "u would wanna kiss me"

MK: "Yes I would;)"

MK: "Is there any where else you would like me to kiss besides your lips?"

UCA2: "like where?"

MK: "Anywhere maybe your nipples and your cookie;)"

MK: "Have you ever touched a boy's penis?"

UCA2: "omg no I havent lol"

MK: "Oh okay"

UCA2: "can you tell me how that would work?"

MK: "What do you mean?"

UCA2: "ive never done it before so idk how"

MK: "Oh okay maybe you could touch mine when we meet and you cuddling in my lap"

MK: "What would you want to do when we go into your bedroom?"

UCA2: "idk where to start really"

UCA2: "what would u do?"

MK: "I would like for you to lay on your stomach and let me explore your back side of your body. Would you like that?"

UCA2: "how would u explore it?"

MK: "Gently touching your back with my hands kissing as I touch you"

MK: "Taking your top off and then your panties"

MK: "After I'm done with your back I would like you to roll onto your back and I would like to explore your front side;)"

UCA2: "what would the exploring be? Like you said before or?"

MK: "kissing you passionately working my way to your breast your nipples getting hard as I touch them and kiss them taking the toy and using it on your nipples working my way down to your belly button kissing you there then working my way to your cookie using the toy you spread your legs wide as I tease you I find your hard clit and touch it

with the toy you say it feels good and tell me not to stop I get down and use my tongue to gently touch your clit until you cum I want to taste your sweet juices."
MK: "You will be surprised how good it feels when you cum;)"

06MAY24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:
MK: "I was thinking of you all weekend. I was thinking how nice it will be laying on your bed and me massaging you all over. I bought some massage oil. I was thinking how exciting to see your cookie and playing you spreading your legs open and you moaning."
MK: "I want to play and kiss your sweet nipples."
MK: "I would love you to touch my hard penis"
UCA2: "id be ok with that if u want..what would touching it feel like tho"
MK: "it would feel awesome you moving your hand up and down would make me cum;)"
MK: "I would tease your clit until you cum. Would love to taste your sweet juices;)"
UCA2: " this might be a weird question lol but can you tell me what a hard penis looks like"
MK: "Would you like to see mine?"
UCA2: "yea id be ok with that if u wanted"

31. On 06MAY24, MARTY LEE KAMINSKI proceeded to send two (2) photographs of an adult male penis to UCA2. Additionally, on 06MAY24, MARTY LEE KAMINSKI sent UCA2 a text message stating "This talks about your clit" and a weblink with the title "Clitoris". The link appeared to be associated with my.clevelandclinic.org.

08MAY24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:
MK: "What would you like? Perfume

UCA2: "I dont really know names of perfumes"

MK: "What do you borrow from your mom?"

UCA2: "I can remember"

UCA2: "cant"

MK: "I asked your mom and she said you like her Victoria Secret"

UCA2: "oh yeah that sounds right lol"

MK: "Is there anything else you would like? Maybe some sexy panties lol"

UCA2: "oh lol my mom just asked me that

UCA2: "…r u only talkin to me bc u like my mom??"

MK: "No I want you Kaylee. I ask her about what she thinks you would like I want to spoil you sweetheart"

UCA2: "r u sure u want me and not my mom?"

MK: "Yes how can I prove that sweetheart?"

MK: "She has told me from the beginning that it's all about you not her"

MK: "I don't even know what your mom looks like I definitely want you Kaylee"

UCA2: "idk I was just checkin"

MK: "What is your favorite color and what size panties do you wear?"

MK: "Have you worn sexy panties?"

UCA2: "my favorite color is purple. I think 10 or 10/12?"

MK: "I really like purple. Have you ever worn a thong?"

MK: "They come in xs and up"

MK: "Something like this"

32. MARTY LEE KAMINSKI proceeded to send UCA2 a weblink with the title "Buy Lace Brazilian Panty." The link appeared to be associated with www.victoriassecret.com. MARTY LEE KAMINSKI indicated he would purchase the items contained within the link for UCA2.

33. On 09MAY24, MARTY LEE KAMINSKI sent text messages to UCA2 stating "Morning beautiful" and "I'm going to Victoria Secret today to get you a sexy

present;)".

34. On 09MAY24, NCIS Special Agents conducted surveillance at the residence of MARTY LEE KAMINSKI located at 402 Brookview Drive, Jacksonville, NC 28540. NCIS Special Agents witnessed MARTY LEE KAMINSKI depart his residence in a white CADILLAC XT5 bearing North Carolina tag "946T DV" and proceed to Jacksonville Mall located at 375 Western Boulevard, Jacksonville, NC. NCIS Special Agents observed MARTY LEE KAMINSKI enter the Victoria's Secret store within the Jacksonville mall. MARTY LEE KAMINSKI was observed inside the Victoria's Secret store purchasing various perfumes and lingerie. Additional surveillance observed MARTY LEE KAMINSKI exit the mall with a pink Victoria's Secret bag.

09MAY24

Conversation between UCA1 and MARTY LEE KAMINSKI (MK) via text message:

MK: *one image depicting 2 lotion bottles and 3 perfume bottles from Victoria's Secret*

MK: *one image depicting 1 purple bra and 3 pairs of purple underwear*

MK: "I spoiled Kaylee today"

13MAY24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:

MK: "Oh just feeling a little insecure but I'm fine. I want to see you wearing your purple panties and bra."

UCA2: "insecure? but why??"

UCA2: "i can do that if u want. what will u wear?"

MK: "What would you like me to wear? Insecure because I don't want to disappoint you."

MK: "I don't have any sexy underwear like you have lol"

UCA2: "what kinda underwear do u have?"

MK: "Let me go into bathroom and I will take a picture"

UCA2: "ooook"

35. MARTY LEE KAMINSKI proceeded to send UCA2 five (5) images in which he indicated were of himself. An adult male penis can be seen in two (2) of the images.

16MAY24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:

MK: "Do you thinnk you would like to touch my penis?"

UCA2: "yeah if u want me to too. id be ok with that"

MK: "That would feel so nice"

UCA2: "do all boys thingys look like urs?"

MK: "Yes and no. I'm circumcised that is were they cut the foreskin off at birth."

36. MARTY LEE KAMINSKI proceeded to send UCA2 a weblink with the title "Circumcision." The link appeared to originate from www.google.com.

37. On 30MAY24, MARTY LEE KAMINSKI sent UCA2 a text message stating "Just got out of the shower thinking of you sweetheart." MARTY LEE KAMINSKI subsequently sent an image of an adult male penis to UCA2.

38. On 06JUN24, NCIS Special Agents conducted a controlled in-person meet with MARTY LEE KAMINSKI and a UCA (UCA) who he believed to be the mother of UCA2. During the interaction, MARTY LEE KAMINSKI disclosed to the UCA he would, "like to see her [UCA2] in the outfits he bought her," which he stated he planned to bring with him when they meet. MARTY LEE KAMINSKI detailed to the UCA he wanted to give UCA2 a massage, play with her nipples and vagina, and planned to bring "the toy" with him when he met UCA2 in person. MARTY LEE KAMINSKI continued describing sexual acts he intended to participate in with UCA2, which included UCA2 touching his penis and him touching UCA2's clitoris.

MARTY LEE KAMINSKI added to the UCA that he was interested in sexual interactions with UCA2 occurring "more than once."

06JUN24

Conversation between UCA2 and MARTY LEE KAMINSKI (MK) via text message:

MK: "It went very well. Your mom asked me about wearing a condom and I said I would. Maybe when the time comes you will help me put it on;)"

UCA2: "oh okay. how would i do that?"

MK: "Help me slide it over my hard penis;)"

MK: "A condom is like a very stretchable ballon."

UCA2: "oh really?? do they come in diff colors like balloons?"

MK: "lol yes they do come in different colors, what color would you like?"

UCA2: "omg really?? do they have purple ones?"

MK: "I will see sweetheart"

39. On 06JUN24, MARTY LEE KAMINSKI proceeded to send UCA2 what appeared to be a screenshot image from "ripnroll.com." The screenshot image depicted "Atlas Rainbow Colors Condoms."

40. On 25JUN24, NCIS received a Priority Mail United States Postal Service package to a pre-established Post Office Box. The package was addressed to "Kaylee Alexander" and displayed return address "402 Brookview Dr, Jacksonville, NC 28540" with associated name "MARTY." The package contained a greeting card with a handwritten note. The note appeared to say: "Kaylee, Sorry that you aren't feeling well. Hope this puts a smile on your face sweetheart. Marty."

41. Throughout the conversations, MARTY LEE KAMINSKI has sent UCA1 and UCA2

various photographs and videos via text message, including but not limited to, photographs of himself, animals, underwear, perfumes, and his residence.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

42. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

43. Electronic storage devices (like cellphones, computers, tablets) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names.

44. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

45. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

46. Searching electronic storage and computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a

"booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

47. In order to fully retrieve data from a computer system and mobile computer devices, the analyst needs all data storage devices, as well as the computer hardware associated with the system. In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/ devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

48. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law should all

be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers, cellphone, tablet computers, mobile computer devices, and related devices consistent with the scope of the requested search.

UNLOCKING BIOMETRICALLY SECURED DEVICES

49. Unlocking the device(s) with biometric features. The warrant I am applying for would permit law enforcement to compel **MARTY LEE KAMINSKI** to unlock (1) any device on **MARTY LEE KAMINSKI**'s person, vehicle and premises; (2) any device found in a backpack or baggage believed to owned, used, or accessed by **MARTY LEE KAMINSKI**; using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that

one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device (such as an iPhone) has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

50. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **MARTY LEE KAMINSKI** to the fingerprint scanner of the seized device(s); (2) hold the device(s) in front of the face of **MARTY LEE KAMINSKI** to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face **MARTY LEE KAMINSKI** and activate the iris recognition feature, for the purpose of attempting to unlock the device(s), and attempting to access data contained in the device, in order to search the contents as authorized by this warrant.

SUMMARY

51. Based upon the above, I believe **MARTY LEE KAMINSKI** communicated with a NCIS UCA between 01May24 and 25Jun24 and committed violations of Title 18, United States Code Section 2422 (Coercion and Enticement of a Minor) and Section 1470 (Transfer of Obscene Materials to Minors) based on the messages and recorded sessions between **MARTY LEE KAMINSKI** and UCAs. I also believe **MARTY LEE KAMINSKI** displays characteristics common to individuals who have a sexual interest in children.

52. Based on my training, knowledge and experience, as well as the documented experience of other investigators, individuals who have a sexual interest in children utilize multiple devices, many of which are portable, such as a smartphone, laptop computer, and external storage devices, such as flash drives, external hard drives, and other storage media. These devices are often kept in the individuals' homes, vehicles, place of employment and on their person.

CONCLUSION

53. Based on the foregoing information, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES as set forth herein and in Attachment B are currently contained in the TARGET LOCATION, more fully described in Attachment A. I therefore respectfully request that search warrants be issued authorizing the search of the TARGET LOCATION described in Attachments A for the items described in Attachment B and authorizing the seizure and examination of any such items found therein.

Special Agent Jamie Smith
Naval Criminal Investigative Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 8 day of July, 2024.

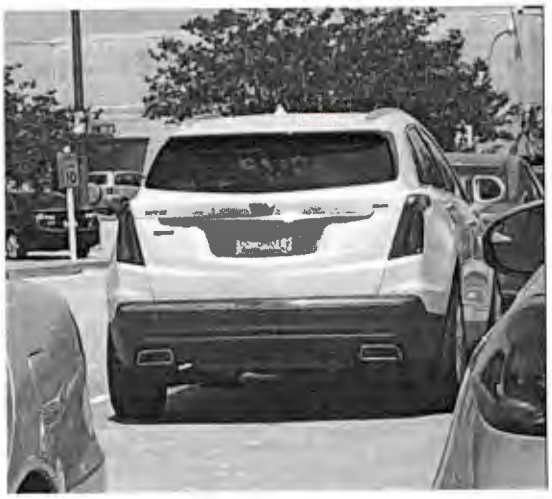
HONORABLE ROBERT B. JONES, JR
UNITED STATES MAGISTRATE JUDGE

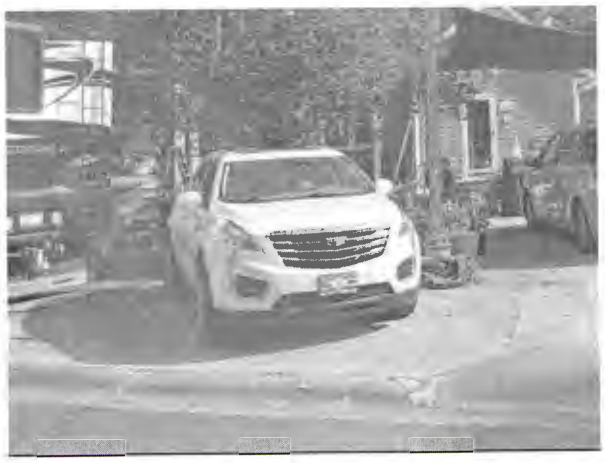
ATTACHMENT A

Description of places to be searched

A **2017 CADILLAC XT5 VIN: 1GYKNBRSXHZ106287** bearing North Carolina Disabled Veteran tag "946T DV".

The photographs below depict the vehicle to be searched.





ATTACHMENT B

List of items to be seized and searched

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 2241(Aggravated Sexual Abuse), the "Target Offenses", including but not limited to:

a. Any and all notes, documents, records, or correspondence, including by U.S. Mails or by computer, pertaining to violations of 18 U.S.C. § 2241;

b. Any mobile device, computer, or electronic storage medium, and any attached memory cards or storage mediums, belonging to or controlled by MARTY LEE KAMINSKI, including but not limited to, cellular phones, tablets, hard drives, SIM cards, SD cards, micro-SD cards, and any other device capable of connecting, or exchanging data with the Internet, found in the locations described within Attachment A;

c. Any items (blankets, sex toys, clothes, perfumes, gifts, etc.) bearing resemblance to items observed in the messages and described within the affidavit;

d. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to the TARGET LOCATION;

e. Any and all diaries, notebooks, notes, address books, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.

2. Any and all images, messages, and communications regarding methods to avoid detection by law enforcement.

3. This authorizes the forensic examination of any cellular phone, tablet, computer, computer hard drive, or other electronic device or physical object upon which computer data can be recorded (hereinafter, "DEVICES") that is called for by this warrant, or that might contain things otherwise called for by this warrant, for the purpose of identifying and securing the following electronically stored information which constitute evidence of the commission of a criminal offense, contraband, the fruits of a crime, namely violations of 18 U.S.C. § 2241(Aggravated Sexual Abuse):

a. evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of the times the DEVICES were used;

c. passwords, encryption keys, and other access devices that may be necessary to access the DEVICES; documentation and manuals that may be necessary to access

the DEVICES or to conduct a forensic examination of the DEVICES;

d. evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

e. evidence of the lack of such malicious software;

f. All phone numbers and associated names or aliases stored within the DEVICES "Contacts" or a stored phone book within the memory of the DEVICES;

g. Any and all communication between MARTY LEE KAMINSKI and UCA1, UCA2 and UCA3, including but not limited to, sent and received text messages, SMS messages, MMS messages, picture files, video files, audio files, emails, all incoming and outgoing phone call logs, and any metadata associated within those files which are stored within the memory of the DEVICES;

h. All picture files or video files, to include recoverable deleted files, stored within the memory of the DEVICES from May 1, 2024 to Present;

i. Records of or information about the DEVICES Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, to include recoverable deleted files, and records of user-typed web addresses from April 30, 2024 to Present;

j. All geolocation data from April 30, 2024 to Present.

5. DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to any digital items subject to seizure pursuant to this warrant; law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of MARTY LEE KAMINSKI to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of MARTY LEE KAMINSKI and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face MARTY LEE KAMINSKI and activate the iris recognition feature, for the purpose of attempting to unlock the device(s), and attempting to access data contained in the device, in order to search the contents as authorized by this warrant.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.